The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
04/05/2016

SUBJECT:
Multiple Vulnerabilities in Google Android OS Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Android operating system (OS), the most severe of which could allow for remote code execution. Android is an operating system developed by Google for mobile devices including, but not limited to smartphones, tablets, and watches. These vulnerabilities could be exploited through multiple methods including email, web browsing and MMS when processing media files. Successful exploitation of these vulnerabilities could result in remote code execution in the context of the application, an attacker gaining elevated privileges, blocking access to a Bluetooth device, or bypassing security restrictions.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
Android OS builds prior to versions 6.0.1 and without Security Patch Levels of April 02, 2016

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:
Google's Android OS is prone to multiple vulnerabilities, the most severe of which could allow for remote code execution. The vulnerabilities are as follows:
- Multiple remote code execution vulnerabilities exist in the 'DHCPCD' client.(CVE-2014-6060, CVE-2016-1503)
- A remote code execution vulnerability in 'Media Codec' service exists when it processes a specially crafted media file. (CVE-2016-0834)

- Multiple remote code execution vulnerabilities in 'Mediaserver' exist when it processes a specially crafted media file. (CVE-2016-0835, CVE-2016-0836, CVE-2016-0837, CVE-2016-0838, CVE-2016-0839, CVE-2016-0840, CVE-2016-0841)
- A remote code execution vulnerability in 'libstagefright' service exists when it processes a specially crafted media file. (CVE-2016-0842)
- An elevation of privilege vulnerability in the 'Kernel' exists that could allow for a local malicious application to execute arbitrary code within the kernal. (CVE-2015-1805, CVE-2014-9322)
- An elevation of privilege vulnerability in the 'Qualcomm Performance Module' exists that could allow for a local malicious application to execute arbitrary code within the kernal. (CVE-2015-1805)
- An elevation of privilege vulnerability in the 'Qualcomm RF' component exists that could allow for a local malicious application to execute arbitrary code within the kernal. (CVE-2016-0844)
- An elevation of privilege vulnerability in the 'IMemory Native Interface' exists that could allow for a local malicious application to execute arbitrary code within the context of an elevated system application. (CVE-2016-0846)
- An elevation of privilege vulnerability in the 'Telecom' component exists that could allow a user to spoof their phone calls, by making them appear to come from any random number. (CVE-2016-0847)
- An elevation of privilege vulnerability in the 'Download Manager' exists that could allow for the access to unauthorized files in private storage. (CVE-2016-0848)
- An elevation of privilege vulnerability in the 'Recovery Procedure' exists that could enable a local malicious application to execute arbitrary code within the context of an elevated system application. (CVE-2016-0849)
- An elevation of privilege vulnerability in 'Bluetooth' exists that could enable an untrusted device to pair with a phone. (CVE-2016-0850)
- An elevation of privilege vulnerability in a 'Texas Instruments Haptic Driver' exists that could enable a local malicious application to execute arbitrary code within the context of the kernel. (CVE-2016-2409)
- An elevation of privilege vulnerability in a 'Qualcomm Video Kernel Driver' exists that could enable a local malicious application to execute arbitrary code within the context of the kernel. (CVE-2016-2410)
- An elevation of privilege vulnerability in a 'Qualcomm Power Management' component exists that could enable a local malicious application to execute arbitrary code within the context of the kernel. (CVE-2016-2411)
- An elevation of privilege vulnerability in 'System_server' exists that could enable a local malicious application to execute arbitrary code within the context of an elevated system application.. (CVE-2016-2412)
- An elevation of privilege vulnerability in 'Mediaserver' exists that could enable a local malicious application to execute arbitrary code within the context of an elevated system application. (CVE-2016-2413)
- A local denial of service vulnerability in the 'Minikin' exists that could allow a local attacker to block access to an affected device. (CVE-2016-2414)
- An information disclosure vulnerability in 'Exchange ActiveSync' exists that could allow an application to access sensitive information. (CVE-2016-2415)
- Multiple information disclosure vulnerabilities in 'Mediaserver' that could allow for a bypass of security measures in place to increase the difficulty of attackers exploiting the platform. (CVE-2016-2416, CVE-2016-2417, CVE-2016-2418, CVE-2016-2419)

- An elevation of privilege vulnerability in the 'Debuggerd' component could enable a local malicious application to execute arbitrary code that could lead to a permanent device compromise. (CVE-2016-2420)
- An elevation of privilege vulnerability in the 'Setup Wizard' exists that could result in the ability to bypass the Factory Reset Protection and gain access to the device. (CVE-2016-2421)
- An elevation of privilege vulnerability in 'Wi-Fi' existsthat could enable a local malicious application to execute arbitrary code within the context of an elevated system application. (CVE-2016-2422)
- An elevation of privilege vulnerability in 'Telephony' existsthat allow an attacker to bypass the Factory Reset Protection and gain access to the device. (CVE-2016-2423)
- A local denial of service vulnerability in 'SyncStorageEngine' exists that could enable a local malicious application to cause a reboot loop. (CVE-2016-2424)
- An information disclosure vulnerability in 'AOSP Mail' exists that could allow a local application to access sensitive information. (CVE-2016-2425)
- An information disclosure vulnerability in the 'Framework' component exists that could allow an application to access sensitive information. (CVE-2016-2426)
- An information disclosure vulnerability in 'BouncyCastle' exists that could allow an authentication key to be leaked. (CVE-2016-2426)

Successful exploitation of these vulnerabilities could result in remote code execution in the context of the application, an attacker gaining elevated privileges, blocking access to a Bluetooth device, or bypassing security restrictions.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Google Android or mobile carriers to vulnerable systems, immediately after appropriate testing.
- Remind users to download apps only from trusted vendors in the Play Store.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Google:

https://source.android.com/security/bulletin/2016-04-02.html

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1503
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6060

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0834
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0835
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0836

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0837
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0838
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0839
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0840
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0841
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0842
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1805
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0843
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0844
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9322
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0846
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0847
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0848
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0849
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0850
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2409
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2410
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2411
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2412
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2413
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2414
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2415
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2416
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2417
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2418
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2419
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2420
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2421
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2422
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2423
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2424
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2425
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2426
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2427